JOURNAL OF ALGEBRA 79, 218–234 (1982)

Relative Invariants of Finite Groups

HARUHISA NAKAJIMA*

Department of Mathematics, Keio University, Yokohama-shi 223, Japan

Communicated by D. Buchsbaum

Received March 9, 1981

1. INTRODUCTION

Let V be a finite-dimensional vector space over a field k of characteristic p ($\geqslant 0$) and G a finite subgroup of $GL(V)$. Then G acts naturally on the symmetric algebra $k[V]$ of V. If χ is a linear character of G (i.e., $\chi \in \mathrm{Hom}(G, k^*)$), we denote by $k[V]_\chi$ the set

$$\{f \in k[V] \mid \sigma(f) = \chi(\sigma) f \quad \text{for} \quad \text{all } \sigma \in G\}$$

whose elements are known as χ-*invariants* (*semiinvariants*, *relative invariants* or *invariants relative to* χ). The ring of invariants $k[V]^G$ is regarded as a graded subalgebra of $k[V]$ with respect to the natural graduation of $k[V]$. Clearly, $k[V]_\chi$ is a finitely generated graded $k[V]^G$-module. By the Galois theory of fields it is easy to see that $k[V]_\chi$ is not a trivial module.

Now let us consider the module structure of $k[V]_\chi$ under the assumption that $k = \mathbb{C}$ ($\mathbb{C}$ denotes the complex number field). We can associate χ with a homogeneous polynomial f_χ of $\mathbb{C}[V]$, where f_χ is effectively determined by the $\mathbb{C}G$-module V and χ (for definition, see Section 3 and [9, Sect. 2]). In [9] Stanley has proved

THEOREM 1.1 (Stanley, cf. [9, (2.3)]). *The following statements on a linear character χ of a finite subgroup G of $GL(V)$ are equivalent:*

(1) *$\mathbb{C}[V]_\chi$ is a graded free $\mathbb{C}[V]^G$-module of rank one.*

(2) *f_χ is a χ-invariant of G.*

If a normal subgroup H of G contains the commutator subgroup $[G, G]$, then there is a subgroup X_H of $\mathrm{Hom}(G, \mathbb{C}^*)$ such that $H = \bigcap_{\chi \in X_H} \mathrm{Ker}\, \chi$. Applying the Reynolds operators, we can show that $\mathbb{C}[V]^H = \bigoplus_{\chi \in X_H} \mathbb{C}[V]_\chi$. Hence, in the case where $\mathbb{C}[V]_\chi$ are free $\mathbb{C}[V]^G$-modules for $\chi \in X_H$, Theorem 1.1 informs us of the ring structure of $\mathbb{C}[V]^H/\mathfrak{n}\mathbb{C}[V]^H$ where $\mathfrak{n}$ is

* Present Address: Department of Mathematics, Tokyo Metropolitan University, Fukazawa, Setagaya-ku, Tokyo 158, Japan.

0021-8693/82/110218-17$02.00/0

the irrelevant maximal ieal of $\mathbb{C}[V]^G$. When G is generated by pseudo-reflections, this viewpoint plays an important role for Stanley to try to classify H such that $\mathbb{C}[V]^H$ is a complete intersection. (In [10] Stanley has conjectured that if $\mathbb{C}[V]^G$ is a complete intersection, then there is a finite group $\tilde{G}$ generated by pseudo-reflections in $GL(V)$ which contains G with $G \supseteqq [\tilde{G}, \tilde{G}]$.)

The proof of Theorem 1.1, which has appeared in [9], depends essentially on the following classical result of Molien.

THEOREM 1.2 (Molien, cf. [5, 2]). *If χ is an element of* $\mathrm{Hom}(G, \mathbb{C}^*)$, *then*

$$\sum_{n=0}^{\infty} \dim(\mathbb{C}[V]_\chi)_n T^n = \frac{1}{|G|} \sum_{\sigma \in G} \frac{\chi(\sigma)^{-1}}{\det(1 - T\sigma)},$$

where $(\mathbb{C}[V]_\chi)_n$ is the graded part of $\mathbb{C}[V]_\chi$ of degree n and T is a variable.

However, this theorem breaks down under the assumption that k has positive characteristic. Thus, we do not have effective criteria for $k[V]_\chi$ to be a free $k[V]^G$-module. The purpose of this paper is to extend the theorem of Stanley to the case where ground fields k are arbitrary. Our proofs were suggested by unpublished results of Professor S. Endo (Tokyo Metropolitan University) in 1974 on divisor class groups of rings of invariants.

The main results in this paper are the following

I (THEOREM 2.9). *Let R be a unique factorization domain such that $U(R) = k^*$ for some subfield k of R and let G be a finite subgroup of* $\mathrm{Aut}(R)$. *Then the following statements on a 1-cocycle $\chi \in Z^1(G, k^*)$ are equivalent:*

(1) *R_χ is a free R^G-module of rank one.*

(2) *There is a unit u_χ of R such that $u_\chi g_\chi \in R_\chi$.*

II (THEOREM 3.1). *If G is a finite subgroup of $GL(V)$, then the following statements on a linear character χ of G are equivalent:*

(1) *$k[V]_\chi$ is a graded free $k[V]^G$-module of rank one.*

(2) *f_χ is a χ-invariant of G.*

III (THEOREM 3.8). *Let G be a finite subgroup of $GL(V)$ and let N be a normal subgroup of G such that G/N is abelian. Suppose that $k[V]^G$ is a polynomial ring and $(|G/N|, p) = 1$ if p $(= \mathrm{char}(k)) > 0$. Then the following statements are equivalent:*

(1) *$k[V]^N$ is a complete intersection.*

(2) *$\rho(N)$ coincides with the group $G_D(k)$ for some datum D.*

Furthermore, we shall give some remarks which are concerned with Samuel's Galois descent (e.g., [7]) and the results of Dress [3] and Kang [4]. For example, we can completely determine finite subgroups G of $GL(V)$ such that all $k[V]_\chi$ are free $k[V]^G$-modules. It should be emphasized that our generalization of Stanley's theorem is useful to compute invariants of finite groups over finite fields.

2. Samuel's Galois Descent and Relative Invariants

For a ring (commutative ring) A, $U(A)$ is defined to be the group of units of A and $\mathscr{P}(A)$ stands for the set of all prime ideals $\mathfrak{p}$ of A with $\mathrm{ht}(\mathfrak{p})$ (height of $\mathfrak{p}$) $= 1$. Moreover, if A is a Krull domain, for an ideal $\mathfrak{a}$ of A we set $\tilde{\mathfrak{a}} = \bigcap_{\mathfrak{p} \in \mathscr{P}(A)} \mathfrak{a}_\mathfrak{p}$ which is called the *divisorialization* of $\mathfrak{a}$ in A and denote by $\mathrm{Cl}(A)$ the divisor class group of A.

We suppose that R is a Krull domain and G is a finite subgroup of $\mathrm{Aut}(R)$. For any prime ideal $\mathfrak{p}$ in $\mathscr{P}(R)$, let $e(\mathfrak{p}, \mathfrak{p} \cap R^G)$ be the ramification index of $\mathfrak{p}$ over $\mathfrak{p} \cap R^G$ (i.e., $(\mathfrak{p} \cap R^G) R_\mathfrak{p} = (\mathfrak{p}R_\mathfrak{p})^{e(\mathfrak{p}, \mathfrak{p} \cap R^G)}$) and let $v_\mathfrak{p}$ be the valuation associated to the discrete valuation ring $R_\mathfrak{p}$ (for a subset B of R, $v_\mathfrak{p}(B)$ satisfies $BR_\mathfrak{p} = (\mathfrak{p}R_\mathfrak{p})^{v_\mathfrak{p}(B)}$). If χ is an element of $Z^1(G, U(R))$ ($Z^1(G, U(R))$ is the group of 1-cocycles of G in $U(R)$), we put

$$R_\chi = \{f \in R \mid \sigma(f) = \chi(\sigma) f \text{ for all } \sigma \in G\},$$

whose elements are called *relative invariants* or *χ-invariants* of G. Then R_χ is an R^G-module.

Lemma 2.1. *The R^G-module R_χ is isomorphic to a divisorial integral ideal of R^G.*

Proof. Let K be the quotient field of R. Then we have $K_\chi \simeq K^G \otimes_{R^G} R_\chi$ and it follows from Hilbert's Theorem 90 that $K_\chi \neq 0$. This implies that $R_\chi \neq 0$ for all $\chi \in Z^1(G, U(R))$. Thus, we can choose a non-zero element f from $R_{\chi^{-1}}$. It is obvious that $\widetilde{fR_\chi R} \cap R^G$ $(= \widetilde{R_\chi R f} \cap R^G) = fR_\chi$. We deduce easily from this that fR_χ is divisorial in R^G (i.e., R_χ is isomorphic to a divisorial integral ideal of R^G) since G is finite.

Lemma 2.2. *For any $\mathfrak{p} \in \mathscr{P}(R)$ we have*

$$v_\mathfrak{p}(R_\chi R) < e(\mathfrak{p}, \mathfrak{p} \cap R^G),$$

where $R_\chi R$ denotes the ideal of R generated by R_χ.

Proof. Let $\mathfrak{p}$ be any prime ideal in $\mathscr{P}(R)$ and put $S = R^G_\mathfrak{q} \otimes_{R^G} R$ where

$\mathfrak{q} = \mathfrak{p} \cap R^G$. Then S is a Krull domain on which G acts naturally and we can identify S_χ with $R_\mathfrak{q}^G \otimes_{R^G} R_\chi$. If $\mathfrak{p}'$ is a prime ideal of S lying over $\mathfrak{q}S^G$, then $\mathfrak{p}'$ is conjugate to $\mathfrak{p}S$ under the action of G. Because $S_\chi S$ is a G-stable ideal, we must have $v_{\mathfrak{p}S}(S_\chi S) = v_{\mathfrak{p}'}(S_\chi S)$. Suppose that $v_\mathfrak{p}(R_\chi R)$ $(= v_{\mathfrak{p}S}(S_\chi S)) > e(\mathfrak{p}, \mathfrak{q})$ $(= e(\mathfrak{p}S, \mathfrak{q}S^G))$. Then we can choose a divisorial integral proper ideal $\mathfrak{a}$ of S^G $(= R^G\mathfrak{q})$ which satisfies $\widetilde{S_\chi S} = \widetilde{\mathfrak{a}S\mathfrak{b}}$ for a divisorial integral ideal $\mathfrak{b}$ of S. Since S^G is a discrete valuation ring, there is a non-unit h of S^G such that $\widetilde{\mathfrak{a}S} = Sh$. S_χ is contained in $\mathfrak{b}h$, and hence we see that $S_\chi \subseteq \bigcap_{i \geq 1} Sh^i = (0)$, which is a contradiction.

Because G acts naturally on $\mathscr{P}(R)$, $\mathscr{P}(R)$ is a disjoint union of G-orbits, which are called *conjugate classes* in $\mathscr{P}(R)$. We fix a set $\mathscr{C}$ consisting of representatives of all conjugate classes in $\mathscr{P}(R)$ and put

$$v(\chi) = (v_\mathfrak{p}(R_\chi R) \bmod e(\mathfrak{p}, \mathfrak{p} \cap R^G))_{\mathfrak{p} \in \mathscr{C}} \in \bigoplus_{\mathfrak{p} \in \mathscr{C}} \mathbb{Z}/e(\mathfrak{p}, \mathfrak{p} \cap R^G)\,\mathbb{Z}$$

for any 1-cocycle χ of G in $U(R)$ ($\mathbb{Z}$ denotes the ring of all integers). Clearly, $R_\chi R = R_\psi R$ if $\chi \equiv \psi \bmod B^1(G, U(R))$ ($B^1(G, U(R))$ is the group of 1-coboundaries of G in $U(R)$), and hence v induces

$$\bar{v}\colon H^1(G, U(R)) \to \bigoplus_{\mathfrak{p} \in \mathscr{C}} \mathbb{Z}/e(\mathfrak{p}, \mathfrak{p} \cap R^G)\,\mathbb{Z}$$

such that $\bar{v}(\chi B^1(G, U(R))) = v(\chi)$ ($H^1(G, U(R))$ is the first cohomology group of a $\mathbb{Z}G$-module $U(R)$). Let $Z_R^1(G, U(R))$ be the set

$$\{\chi \in Z^1(G, U(R)) \mid R_\chi \nsubseteq \mathfrak{p} \text{ for all } \mathfrak{p} \in \mathscr{P}(R)\},$$

which is a subgroup of $Z^1(G, U(R))$. Since $Z_R^1(G, U(R))$ contains $B^1(G, U(R))$, we can put $H_R^1(G, U(R)) = Z_R^1(G, U(R))/B^1(G, U(R))$.

LEMMA 2.3. *The sequence*

$$0 \to H_R^1(G, U(R)) \to H^1(G, U(R)) \xrightarrow[\bar{v}]{} \bigoplus_{\mathfrak{p} \in \mathscr{C}} \mathbb{Z}/e(\mathfrak{p}, \mathfrak{p} \cap R^G)\,\mathbb{Z}$$

is an exact sequence of groups.

Proof. It suffices to show that

$$v_\mathfrak{p}(R_\chi R R_\psi R) \equiv v_\mathfrak{p}(R_{\chi\psi} R) \bmod e(\mathfrak{p}, \mathfrak{p} \cap R^G)$$

for $\chi, \psi \in Z^1(G, U(R))$ and $\mathfrak{p} \in \mathscr{P}(R)$. As in the proof of Lemma 2.2, we may assume that R^G is a discrete valuation ring. Then, by Lemma 2.1, there are elements f, g, h in R such that $R_\chi = R^G f$, $R_\psi = R^G g$ and $R_{\chi\psi} = R^G h$.

Clearly, $fg \in R_{\chi\psi}$ and so we have $fg = h'h$ for some $h' \in R^G$, which implies that $v_{\mathfrak{p}}(R_\chi R R_\psi R) \equiv v_{\mathfrak{p}}(R_{\chi\psi} R) \bmod e(\mathfrak{p}, \mathfrak{p} \cap R^G)$.

We denote by $[\mathfrak{a}]$ the class of a divisorial ideal $\mathfrak{a}$ in the divisor class group. Let $\varphi\colon \mathrm{Cl}(R^G) \to \mathrm{Cl}(R)$ be a homomorphism such that $\varphi([\mathfrak{a}]) = [\widetilde{\mathfrak{a}R}]$ for each divisorial integral ideal $\mathfrak{a}$ of R^G. We have already known that $\operatorname{Ker}\varphi$ can be embedded in $H^1(G, U(R))$ (e.g., [7]).

LEMMA 2.4. *$\operatorname{Ker}\varphi$ is naturally isomorphic to $H^1_R(G, U(R))$. Moreover φ is injective if and only if R_χ are free R^G-modules for all $\chi \in Z^1_R(G, U(R))$.*

Proof. Let $\mathfrak{a}$ be a divisorial integral ideal of R^G which satisfies $\widetilde{\mathfrak{a}R} = Rf$ for an element f of R. Then there is a 1-cocycle χ of G in $U(R)$ such that f is a χ^{-1}-invariant. Because G is finite and $\mathfrak{a}$ is divisorial, we must have $\mathfrak{a} = \widetilde{\mathfrak{a}R} \cap R^G = fR_\chi$ (to prove this we need only to show that $\mathfrak{a}_{\mathfrak{p}\cap R^G} = \mathfrak{a}R_{\mathfrak{p}} \cap R^G_{\mathfrak{p}\cap R^G}$ for all $\mathfrak{p} \in \mathscr{P}(R)$). Thus, χ belongs to $Z^1_R(G, U(R))$. Conversely, for any $\chi \in Z^1_R(G, U(R))$ and for a non-zero element f of $R_{\chi^{-1}}$, fR_χ is a divisorial integral ideal (cf. Lemma 2.1) whose class belongs to $\operatorname{Ker}\varphi$. Hence, we get a natural isomorphism $H^1_R(G, U(R)) \simeq \operatorname{Ker}\varphi$. The last assertion of Lemma 2.4 follows from this isomorphism and Lemma 2.1.

Now we assume that R is factorial (i.e., R is a unique factorization domain) and fix a set $\mathscr{M} = \{M_{\mathfrak{p}} \mid \mathfrak{p} \in \mathscr{P}(R)\}$ consisting of $M_{\mathfrak{p}} \in R$ which satisfies $RM_{\mathfrak{p}} = \mathfrak{p}$. If $\mathscr{a} = (a_{\mathfrak{p}})_{\mathfrak{p}\in\mathscr{C}}$ is a sequence such that each $a_{\mathfrak{p}}$ is a non-negative integer with $a_{\mathfrak{p}} < e(\mathfrak{p}, \mathfrak{p} \cap R^G)$, we put

$$F(\mathscr{a}) = \prod_{\mathfrak{p}\in\mathscr{C}} \Bigl(\prod_{\mathfrak{q}\in G\mathfrak{p}} M_{\mathfrak{q}}\Bigr)^{a_{\mathfrak{p}}}$$

where $G\mathfrak{p}$ is the G-orbit of $\mathfrak{p}$. Since almost all $a_{\mathfrak{p}}$ are zero, $F(\mathscr{a})$ is well defined. Obviously $F(\mathscr{a})$ is a relative invariant of G and then $\chi_{\mathscr{a}}$ denotes the 1-cocycle which satisfies $R_{\chi_{\mathscr{a}}} \ni F(\mathscr{a})$.

PROPOSITION 2.5. *The homomorphism*

$$\bar{v}\colon H^1(G, U(R)) \to \bigoplus_{\mathfrak{p}\in\mathscr{C}} \mathbb{Z}/e(\mathfrak{p}, \mathfrak{p}\cap R^G)\,\mathbb{Z}$$

is surjective and the following conditions on $\chi \in Z^1(G, U(R))$ are equivalent:

(1) *R_χ is a free R^G-module.*

(2) *$\chi/\chi_{\mathscr{a}}$ belongs to $B^1(G, U(R))$ for some sequence $\mathscr{a} = (a_{\mathfrak{p}})_{\mathfrak{p}\in\mathscr{C}}$ such that each $a_{\mathfrak{p}}$ is a non-negative integer with $a_{\mathfrak{p}} < e(\mathfrak{p}, \mathfrak{p}\cap R^G)$.*

Proof. For $\mathfrak{q} \in \mathscr{C}$ with $e(\mathfrak{q}, \mathfrak{q}\cap R^G) > 1$, let $\mathscr{b}(\mathfrak{q}) = (b_{\mathfrak{p}}(\mathfrak{q}))_{\mathfrak{p}\in\mathscr{C}}$ be a sequence defined by $b_{\mathfrak{p}}(\mathfrak{q}) = 0$ $(\mathfrak{p} \neq \mathfrak{q})$ and $b_{\mathfrak{q}}(\mathfrak{q}) = 1$. Further we put $F_{\mathfrak{q}} = F(\mathscr{b}(\mathfrak{q}))$ and $\chi_{\mathfrak{q}} = \chi_{\mathscr{b}(\mathfrak{q})}$, respectively. Then $0 \leqslant v_{\mathfrak{p}}(R_{\chi_{\mathfrak{q}}}R) \leqslant v_{\mathfrak{p}}(F_{\mathfrak{q}})$ and $v_{\mathfrak{p}}(R_{\chi_{\mathfrak{q}}}R) = v_{\mathfrak{p}'}(R_{\chi_{\mathfrak{q}}}R)$ for $\mathfrak{p}, \mathfrak{p}' \in \mathscr{P}(R)$ with $G\mathfrak{p} = G\mathfrak{p}'$. Put $S = R^G_{\mathfrak{q}\cap R^G} \otimes_{R^G} R$

and suppose that $v_{\mathfrak{q}}(R_{\chi_{\mathfrak{q}}}R)=0$. Since S^G is a discrete valuation ring, $S_{\chi_{\mathfrak{q}}}=S^G g$ for some $g\in S$, and by the assumption $v_{\mathfrak{q}S}(S_{\chi_{\mathfrak{q}}}S)=0$ we must have $g\in U(S)$. This implies that

$$1=v_{\mathfrak{q}S}(g^{-1}F_{\mathfrak{q}})\geqslant v_{\mathfrak{q}S}((\mathfrak{q}S\cap S^G)\,S)=e(\mathfrak{q},\mathfrak{q}\cap R^G),$$

which is a contradiction. Therefore, we see that $\widetilde{R_{\chi_{\mathfrak{q}}}R}=RF_{\mathfrak{q}}$, and it follows from the definition of $\chi_{\mathfrak{q}}$ that

$$R_{\chi_{\mathfrak{q}}}=R_{\chi_{\mathfrak{q}}}\cap(\widetilde{R_{\chi_{\mathfrak{q}}}R})=R^G F_{\mathfrak{q}}$$

for all $\mathfrak{q}\in\mathscr{C}$. If $\alpha=(a_{\mathfrak{p}})_{\mathfrak{p}\in\mathscr{C}}$ is a sequence such that each $a_{\mathfrak{p}}$ is a non-negative integer with $a_{\mathfrak{p}}<e(\mathfrak{p},\mathfrak{p}\cap R^G)$, then we have $F(\alpha)=\prod_{\mathfrak{q}\in\mathscr{C}}F_{\mathfrak{q}}^{a_{\mathfrak{q}}}$ and $\chi_{\alpha}=\prod_{\mathfrak{q}\in\mathscr{C}}\chi_{\mathfrak{q}}^{a_{\mathfrak{q}}}$. Furthermore $v_{\mathfrak{p}}(R_{\chi_{\alpha}}R)=v_{\mathfrak{p}}(F(\alpha))$, because $R_{\chi_{\mathfrak{q}}}=R^G F_{\mathfrak{q}}$ and $\bar{v}$ is a homomorphism (cf. Lemma 2.3). Thus, $\bar{v}$ is surjective and the implication (2) $\Rightarrow$ (1) follows. Let χ be a 1-cocycle of G in $U(R)$ such that R_χ is a free R^G-module and put $a_{\mathfrak{p}}=v_{\mathfrak{p}}(R_\chi R)$ for $\mathfrak{p}\in\mathscr{C}$. Since $\operatorname{rank}_{R^G}R_\chi$ (rank of the R^G-module R_χ) $=1$, we can choose a generator g of R. Then there is a unit u of R such that $ug=F(\alpha)$ where $\alpha=(a_{\mathfrak{p}})_{\mathfrak{p}\in\mathscr{C}}$ and therefore χ/χ_{α} is a 1-coboundary of G in $U(R)$. The proof of Proposition 2.5 is completed.

Hereafter we assume that there is a subfield k of R of characteristic p ($\geqslant 0$) such that $U(R)=k^*$ ($=U(k)$). We say that an automorphism σ of R is a *generalized reflection* of $\operatorname{Aut}(R)$ if $(\sigma-1)R\subseteq\mathfrak{p}$ for some $\mathfrak{p}\in\mathscr{P}(R)$. It should be noted that all generalized reflections of $\operatorname{Aut}(R)$ are k-algebra automorphisms. For each $\mathfrak{p}\in\mathscr{P}(R)$, let $I_{\mathfrak{p}}$ denotes the inertia group of $\mathfrak{p}$ under the natural action of G, i.e., $I_{\mathfrak{p}}=\{\sigma\in G\mid(\sigma-1)R\subseteq\mathfrak{p}\}$. Because $H^1(I_{\mathfrak{p}},k^*)=\operatorname{Hom}(I_{\mathfrak{p}},k^*)$ and $\mathfrak{p}=RM_{\mathfrak{p}}$ is $I_{\mathfrak{p}}$-stable, $\delta_{\mathfrak{p}}\colon I_{\mathfrak{p}}\to k^*$ defined by $\delta_{\mathfrak{p}}(\sigma)=\sigma(M_{\mathfrak{p}})/M_{\mathfrak{p}}$ (for $\sigma\in I_{\mathfrak{p}}$) is a homomorphism of groups.

LEMMA 2.6. *For $\mathfrak{p}\in\mathscr{P}(R)$ the order of the group $I_{\mathfrak{p}}/\operatorname{Ker}\delta_{\mathfrak{p}}$ is equal to $e(\mathfrak{p},\mathfrak{p}\cap R^G)$ and $\operatorname{Hom}(I_{\mathfrak{p}},k^*)$ is a cyclic group generated by $\delta_{\mathfrak{p}}$.*

Proof. Since $M_{\mathfrak{p}}^{|I_{\mathfrak{p}}/\operatorname{Ker}\delta_{\mathfrak{p}}|}\in R^{I_{\mathfrak{p}}}$ and $\mathfrak{p}\cap R^{I_{\mathfrak{p}}}$ is unramified over $\mathfrak{p}\cap R^G$, we can easily show that $|I_{\mathfrak{p}}/\operatorname{Ker}\delta_{\mathfrak{p}}|\geqslant e(\mathfrak{p},\mathfrak{p}\cap R^{I_{\mathfrak{p}}})=e(\mathfrak{p},\mathfrak{p}\cap R^G)$ and $uM_{\mathfrak{p}}^{e(\mathfrak{p},\mathfrak{p}\cap R^G)}\in R^{I_{\mathfrak{p}}}$ for some $u\in R$ with $u\notin\mathfrak{p}$. Clearly, u is a relative invariant of $I_{\mathfrak{p}}$. If there is an element σ in $I_{\mathfrak{p}}$ such that $\sigma(u)\neq u$, then $\sigma(u)-u=cu$ for some $c\in k^*$ and so u is divisible by $M_{\mathfrak{p}}$. Thus, we must have $u\in R^{I_{\mathfrak{p}}}$ and $e(\mathfrak{p},\mathfrak{p}\cap R^G)=e(\mathfrak{p},\mathfrak{p}\cap R^{I_{\mathfrak{p}}})=|I_{\mathfrak{p}}/\operatorname{Ker}\delta_{\mathfrak{p}}|$. From the classical ramification theory of discrete valuation rings we deduce that $\operatorname{Ker}\delta_{\mathfrak{p}}$ is a p-group if $\operatorname{char}(k)=p>0$. In the case of $p=0$, $\operatorname{Ker}\delta_{\mathfrak{p}}$ is trivial and hence we always have $\operatorname{Hom}(I_{\mathfrak{p}}/\operatorname{Ker}\delta_{\mathfrak{p}},k^*)\cong\operatorname{Hom}(I_{\mathfrak{p}},k^*)$, which is generated by $\delta_{\mathfrak{p}}$.

If $\chi\in Z^1(G,U(R))$ and $\mathfrak{p}\in\mathscr{P}(R)$, then by Lemma 2.6 we can put

$$t_{\mathfrak{p}}(\chi)=\min\{n\in\mathbb{Z}_+\mid\chi(\sigma)=\delta_{\mathfrak{p}}(\sigma)^n\text{ for all }\sigma\in I_{\mathfrak{p}}\},$$

where $\mathbb{Z}_+$ is the set of all non-negative integers.

PROPOSITION 2.7. *For any $\chi \in Z^1(G, U(R))$ and $\mathfrak{p} \in \mathscr{P}(R)$, $t_\mathfrak{p}(\chi)$ is equal to $v_\mathfrak{p}(R_\chi R)$.*

Proof. We fix a prime ideal $\mathfrak{p}$ in $\mathscr{P}(R)$ and put $S = R^G_{\mathfrak{p}\cap R^G} \otimes_{R^G} R$. Since S^G is a discrete valuation ring, there is an element g of S which generates S_χ as an S^G-module. We choose g' from S such that $g = g' M_\mathfrak{p}^{v_{\mathfrak{p}S}(S_\chi S)}$. Then $\sigma(g')/g' = \delta_\mathfrak{p}(\sigma)^{t_\mathfrak{p}(\chi) - v_{\mathfrak{p}S}(S_\chi S)}$ for all $\sigma \in I_\mathfrak{p}$. If $\sigma(g') \neq g'$ for some $\sigma \in I_\mathfrak{p}$, g' is divisible by $M_\mathfrak{p}$ in S, which is a contradiction. Thus, $\delta_\mathfrak{p}^{t_\mathfrak{p}(\chi)} = \delta_\mathfrak{p}^{v_\mathfrak{p}(R_\chi R)}$, and so it follows from Lemma 2.2 that $t_\mathfrak{p}(\chi) = v_\mathfrak{p}(R_\chi R)$.

By Lemmas 2.3 and 2.6 and Proposition 2.7 we see that

$$Z^1(G, k^*) \ni \chi \longmapsto \delta_\mathfrak{p}^{t_\mathfrak{p}(\chi)} \in \mathrm{Hom}(I_\mathfrak{p}, k^*)$$

are homomorphisms for all $\mathfrak{p} \in \mathscr{C}$, and hence they induce the homomorphism

$$t: H^1(G, k^*) \to \bigoplus_{\mathfrak{p} \in \mathscr{C}} \mathrm{Hom}(I_\mathfrak{p}, k^*)$$

in the natural way.

COROLLARY 2.8. *The sequence*

$$0 \to H^1_R(G, k^*) \to H^1(G, k^*) \xrightarrow[t]{} \bigoplus_{\mathfrak{p} \in \mathscr{C}} \mathrm{Hom}(I_\mathfrak{p}, k^*) \to 0$$

is exact, and t is an isomorphism if and only if R^G is factorial.

Proof. By Lemma 2.6 we get a commutative diagram

$$\begin{tikzcd}
 & \bigoplus_{\mathfrak{p} \in \mathscr{C}} \mathrm{Hom}(I_\mathfrak{p}, k^*) \arrow[dd, phantom, "\wr\|"] \\
H^1(G, k^*) \arrow[ur, "t"] \arrow[dr, "\bar{v}"'] & \\
 & \bigoplus_{\mathfrak{p} \in \mathscr{C}} \mathbb{Z}/e(\mathfrak{p}, \mathfrak{p} \cap R^G)\mathbb{Z}
\end{tikzcd}$$

Thus this corollary follows from Lemmas 2.3 and 2.4.

Since almost all $t_\mathfrak{p}(\chi)$ are zero, we can put

$$g_\chi = \prod_{\mathfrak{p} \in \mathscr{P}(R)} M_\mathfrak{p}^{t_\mathfrak{p}(\chi)}.$$

THEOREM 2.9. *The following statements on a 1-cocycle χ of G in k^* are equivalent:*

(1) *R_χ is a free R^G-module.*

(2) *There is an element u_χ in k^* such that $u_\chi g_\chi$ is a χ-invariant of G.*

If these equivalent conditions are satisfied, then we have $R_\chi = R^G u_\chi g_\chi$.

Proof. By Proposition 2.7 we see that $\widetilde{R_\chi R} = Rg_\chi$. If R_χ is a free R^G-module, then $R_\chi = R^G h$ for some $h \in R$, which implies (2). Conversely we suppose that $u_\chi g_\chi \in R_\chi$ for some $u_\chi \in k^*$. Since R_χ is contained in $Ru_\chi g_\chi$, we must have $R_\chi = R^G u_\chi g_\chi$.

For a group H we put $X_k(H) = \mathrm{Hom}(H, k^*)$ and

$$\mathscr{D}_k(H) = \bigcap_{\chi \in X_k(H)} \operatorname{Ker} \chi$$

respectively and, for a ring A, denote by AH the group ring of H over A. If H is a finite group, we have $\mathscr{D}_k(X_k(H)) = \{1\}$ and $|X_k(H)| = |H/\mathscr{D}_k(H)|$. Consequently, if

$$0 \to H_1 \to H_2 \to H_3 \to 0$$

is an exact sequence of finite abelian groups such that $\mathscr{D}_k(H_1) = \mathscr{D}_k(H_2) = \{1\}$, then the sequence

$$0 \to X_k(H_3) \to X_k(H_2) \to X_k(H_1) \to 0$$

is also exact.

LEMMA 2.10. *Suppose that G acts trivially on k. Then we have*

$$R^{\mathscr{D}_k(G)} \cong \bigoplus_{\chi \in X_k(G)} R_\chi$$

as $R^G G/\mathscr{D}_k(G)$-modules.

Proof. Let $\Phi_\chi: R^{\mathscr{D}_k(G)} \to R_\chi$ be the Reynolds operator defined by

$$\Phi_\chi(y) = \frac{1}{|G/\mathscr{D}_k(G)|} \sum_{\sigma \mathscr{D}_k(G) \in G/\mathscr{D}_k(G)} \chi^{-1}(\sigma)\, \sigma(y)$$

for $y \in R^{\mathscr{D}_k(G)}$ (notice that $|G/\mathscr{D}_k(G)|$ is a unit of R). Since $R^{\mathscr{D}_k(G)}$ contains R_χ and $\Phi_\chi(R_\psi) = 0$ for $\chi, \psi \in X_k(G)$ with $\chi \neq \psi$, the $R^G G/\mathscr{D}_k(G)$-homomorphism

$$\Phi: R^{\mathscr{D}_k(G)} \ni x \mapsto (\Phi_\chi(x)) \in \bigoplus_{\chi \in X_k(G)} R_\chi$$

is surjective. It follows from $|G/\mathscr{D}_k(G)| = |\mathrm{Hom}(G, k^*)|$ that $\operatorname{Ker} \Phi$ is a torsion R^G-module. Because $R^{\mathscr{D}_k(G)}$ is a torsion-free R^G-module, Φ is an isomorphism.

Let $\mathscr{R}(G)$ be the subgroup of G generated by all generalized reflections in G ($\mathscr{R}(G)$ is a normal subgroup of G).

THEOREM 2.11. *Suppose that G acts trivially on k. Then the following conditions are equivalent:*

(1) *R^G is a unique factorization domain.*

(2) *$X_k(G/\mathscr{R}(G))$ is trivial.*

(3) *For all $\chi \in X_k(G)$, R_χ are free R^G-modules.*

(4) *$R^{\mathscr{D}_k(G)}$ is a free $R^G G/\mathscr{D}_k(G)$-module.*

(5) *$G = \mathscr{R}(G)\mathscr{D}_k(G)$ (i.e., $G = \{\sigma\tau \mid \sigma \in \mathscr{R}(G), \tau \in \mathscr{D}_k(G)\}$).*

Proof. The equivalence $(1) \Leftrightarrow (3)$ follows from Lemma 2.4, and the implication $(5) \Rightarrow (2)$ is obvious. To prove $(1) \Leftrightarrow (2)$ we need only to show that $H^1_R(G, k^*) \cong X_k(G/\mathscr{R}(G))$ (cf. Lemma 2.4). By Corollary 2.8 we see that $H^1_R(G, k^*) \cong \operatorname{Ker} t \cong X_k(G/\mathscr{R}(G))$.

$(2) \Rightarrow (5)$: It follows from the assumption $X_k(G/\mathscr{R}(G)) = \{1\}$ that the natural homomorphism $X_k(G) \to X_k(\mathscr{R}(G))$ is injective. Hence, we get a commutative diagram

$$\begin{tikzcd}
0 & & \\
X_k(X_k(\mathscr{R}(G))) \arrow[u] \arrow[r] & X_k(X_k(G)) \arrow[r] & 0 \\
\mathscr{R}(G) \arrow[u, "\text{can.}"] \arrow[r, "\text{can.}"'] & G/\mathscr{D}_k(G) \arrow[u, equal, "\wr"', "\text{can.}"] \arrow[r] & 0
\end{tikzcd}$$

of groups with exact rows and an exact column (for convenience we use 0 instead of 1 in this diagram). Thus, we must have $G = \mathscr{R}(G)\mathscr{D}_k(G)$.

$(4) \Rightarrow (3)$: We suppose that $R^{\mathscr{D}_k(G)} = \bigoplus_{\tau \in G/\mathscr{D}_k(G)} R^G \tau(f)$ for some $f \in R^{\mathscr{D}_k(G)}$. Since $kG/\mathscr{D}_k(G) \cong \sum_{\tau \in G/\mathscr{D}_k(G)} k\tau(f)$ as $kG/\mathscr{D}_k(G)$-modules, there is an R^G-basis $\{h_\chi \mid \chi \in X_k(G)\}$ of $R^{\mathscr{D}_k(G)}$ such that h_χ is a χ-invariant of G. From this we easily deduce that all R_χ are free R^G-modules of rank one.

$(3) \Rightarrow (4)$: We can assume that $R_\chi = R^G h_\chi$ for some $h_\chi \in R_\chi$ and identify the $R^G G/\mathscr{D}_k(G)$-module $R^{\mathscr{D}_k(G)}$ with $\bigoplus_{\chi \in X_k(G)} R_\chi$. Then the $kG/\mathscr{D}_k(G)$-module $\sum_{\chi \in X_k(G)} kh_\chi$ is isomorphic to the group ring of $G/\mathscr{D}_k(G)$ over k. Hence $\sum_{\chi \in X_k(G)} kh_\chi = \bigoplus_{\tau \in G/\mathscr{D}_k(G)} k\tau(f)$ for some $f \in R^{\mathscr{D}_k(G)}$ and we must have $R^{\mathscr{D}_k(G)}$ $(= \bigoplus_{\tau \in G/\mathscr{D}_k(G)} R^G\tau(f)) \cong R^G G/\mathscr{D}_k(G)$.

For a finite group H we denote by H^{ab} the commutator quotient of H and by H_q a Sylow q-subgroup of H if q is a prime number. If $q = 0$, we put $H_q = \{1\}$.

COROLLARY 2.12. *Suppose that k is algebraically closed and G acts trivially on k. Let H be a minimal normal subgroup of G such that $|G/H| \in k^*$ and G/H is a solvable group. Then R^G is a unique factorization domain if and only if $G = \mathscr{R}(G)\,H$.*

Proof. Put $D^0(G) = G$ and for any natural number i let $D^i(G) = \mathscr{D}_k(D^{i-1}(G))$. Since k is algebraically closed, $D^i(G)$ is equal to the kernel of the homomorphism $\Psi_i: D^{i-1}(G) \to D^{i-1}(G)^{ab}/(D^{i-1}(G)^{ab})_p$ which is the composite of canonical homomorphism $D^{i-1}(G) \to D^{i-1}(G)^{ab}$, $D^{i-1}(G)^{ab} \to D^{i-1}(G)^{ab}/(D^{i-1}(G)^{ab})_p$. Thus, $D^n(G) = H$ for a sufficiently large n and so it suffices to show that if $G = \mathscr{R}(G)\,D^i(G)$, then $G = \mathscr{R}(G)\,D^{i+1}(G)$ (cf. Theorem 2.11). Using $D^i(G) = \operatorname{Ker} \Psi_i$ we can easily prove this.

PROPOSITION 2.13. *Suppose that R is a noetherian polynomial ring over k and G acts trivially on k. If R^G is a regular ring, then $G = \mathscr{R}(G)\,H$ and R^G is a unique factorization domain. Here H is a minimal normal subgroup of G such that $|G/H| \in k^*$.*

Proof. Assume that R^G is a regular ring and let σ be any element of G such that the order of σ is not divisible by p if $\operatorname{char}(k) = p > 0$. To prove Proposition 2.13 we need only to show that σ belongs to $K = \mathscr{R}(G)\,H$. Let $\bar{k}$ be the algebraic closure of k and let us extend the action of G to the polynomial ring $\bar{k} \otimes_k R$ in the natural way. Then, by the theorem of Bialynicki–Birula (cf. [1; 4, (4.1)]), we can choose a maximal ideal $\bar{\mathfrak{m}}$ of $\bar{k} \otimes_k R$ such that $\sigma(\bar{\mathfrak{m}}) = \bar{\mathfrak{m}}$. Let $\bar{N}$ be the inertia group of $\mathfrak{m}$ under the action of G/K on R^K and put $N = \gamma^{-1}(\bar{N})$ where $\mathfrak{m} = \bar{\mathfrak{m}} \cap R^K$ and γ denotes the canonical homomorphism $G \to G/K$. Because $\bar{\mathfrak{m}}$ is $\langle\sigma\rangle$-stable and σ acts trivially on $\bar{k}$, σ belongs to N. For any prime ideal $\mathfrak{p} \in \mathscr{P}(R)$, K contains the inertia group of $\mathfrak{p}$ under the action of N and hence every divisorial prime ideal of $R^K_{\mathfrak{m}}$ is unramified over $R^N_{\mathfrak{m} \cap R^N}$ (e.g., [6, (41.2)]). Since $R^N_{\mathfrak{m} \cap R^N}$ is unramified over $R^G_{\mathfrak{m} \cap R^G}$ (e.g., [6, (41.2)]), $R^N_{\mathfrak{m} \cap R^N}$ is a regular local ring. Thus, by the purity of branch loci (e.g., [6, (41.1)]), $R^K_{\mathfrak{m}}$ is unramified over $R^N_{\mathfrak{m} \cap R^N}$. Because $\bar{N}$ acts trivially on $R^K/\mathfrak{m}$, we have

$$R^K_{\mathfrak{m}}/\mathfrak{m} R^K_{\mathfrak{m}} = R^N_{\mathfrak{m} \cap R^N}/(\mathfrak{m} \cap R^N)\, R^N_{\mathfrak{m} \cap R^N}.$$

It is well known that R^K is a finitely generated R^N-module and so $R^K_{\mathfrak{m}}$ is also a finitely generated $R^N_{\mathfrak{m} \cap R^N}$-module. Therefore, by Nakayama's lemma, we must have $R^N_{\mathfrak{m} \cap R^N} = R^K_{\mathfrak{m}}$, which implies that $K = N \ni \sigma$. (The last assertion of Proposition 2.13 follows from Theorem 2.11.)

Kan [4] has already proved the last assertion of this proposition.

Remark 2.14. Some of the results in this section can be extended to the case where G is not finite. For example, we note only the following assertion: *With the notation of Theorem* 2.11, *if $G = \mathscr{R}(G)\,\mathscr{D}_k(G)$, then R_χ are free R^G-*

modules for all $\chi \in X_k(G)$ such that $R_\chi \neq 0$ and R^G is a unique factorization domain (*we do not assume that G is finite*).

3. Stanley's Theorem and Applications

In this section we adopt the following notation and terminology: Let R be the symmetric algebra $k[V]$ of a finite-dimensional vector space V over a field k of characteristic p ($\geqslant 0$) and let G be a finite subgroup of $GL(V)$. Then G acts naturally on R as automorphisms of a k-algebra. A subspace U of V^* with $\dim V^*/U = 1$ is called a *reflecting hyperplane relative to* G, if there is a non-unipotent element σ of G with $V^{*\langle\sigma\rangle}$ $(= \{x \in V^* \mid \sigma(x) = x\}) = U$, where V^* is the dual kG-module $\mathrm{Hom}(V, k)$ of V. Let $\mathscr{U} = \{U_i \mid 1 \leqslant i \leqslant n\}$ be the set consisting of all reflecting hyperplanes in V^* relative to G. For each i the set $\mathscr{T}_i = \{\sigma \in G \mid V^{*\langle\sigma\rangle} \supsetneqq U_i\}$ forms a group which contains a normal subgroup $\mathscr{E}_i$ such that $\mathscr{E}_i$ is unipotent on V and $\mathscr{T}_i/\mathscr{E}_i$ is a cyclic group with $|\mathscr{T}_i/\mathscr{E}_i| \in k^*$. The cardinalities $e_i = |\mathscr{T}_i/\mathscr{E}_i|$ ($1 \leqslant i \leqslant n$) are known as *orders of pseudo-reflections in* G (recall that an element $\sigma \in GL(V)$ with $\dim(\sigma - 1)V \leqslant 1$ is called a *pseudo-reflection*). Reflecting hyperplanes U_i, U_j in $\mathscr{U}$ are said to be *equivalent* (in this case we write $U_i \sim U_j$), if U_i is conjugate to U_j under the canonical action of G on the dual module V^*. Exchanging the labels of hyperplanes, we may assume that $\{U_i \mid 1 \leqslant i \leqslant m\}$ is the set of all inequivalent reflecting hyperplanes relative to G. We naturally regard any element of V as a k-linear homomorphism from V^* to k and, for $1 \leqslant i \leqslant n$, choose L_i from V such that $U_i = \{h \in V^* \mid L_i(h)(= h(L_i)) = 0\}$. Clearly, kL_i is $\mathscr{T}_i$-stable, and kL_i is conjugate to kL_j under the natural action of G if and only if U_i is equivalent to U_j. For a linear character $\chi \in X_k(G)$ we put

$$s_i(\chi) = \inf\{r \in \mathbb{Z}_+ \mid \chi(\sigma) = (\det \sigma)^r \text{ for all } \sigma \in \mathscr{T}_i\}.$$

Finally f_χ denotes the homogeneous polynomial

$$\prod_{1 \leqslant i \leqslant n} L_i^{s_i(\chi)}$$

in R.

THEOREM 3.1. *The following statements on a linear character $\chi \in X_k(G)$ of G are equivalent:*

(1) *R_χ is a free R^G-module of rank one.*

(2) *f_χ is a χ-invariant of G.*

If these equivalent conditions (1), (2) *are satisfied, then we have $R_\chi = R^G f_\chi$.*

Proof. For a prime ideal $\mathfrak{p}$ of R let $\mathfrak{p}^*$ be the homogeneous prime ideal

$$\sum_{x \in \mathfrak{p} \cap V} Rx.$$

Then H is equal to H^* if H (resp. H^*) denotes the inertia group of $\mathfrak{p}$ (resp. $\mathfrak{p}^*$) (under the action of G). Therefore, if $\mathfrak{p}$ is a divisorial prime ideal of R and the inertia group of $\mathfrak{p}$ is not trivial, $\mathfrak{p}$ is generated by an element of V. Since

$$\begin{aligned} \mathscr{T}_i &= \{\sigma \in G \mid (\sigma - 1) V \subsetneq kL_i\} \\ &= \{\sigma \in G \mid (\sigma - 1) R \subsetneq RL_i\}, \end{aligned}$$

we deduce from Lemma 2.6 that $e_i = e(RL_i, RL_i \cap R^G)$ and

$$\{\mathfrak{p} \in \mathscr{P}(R) \mid e(\mathfrak{p}, \mathfrak{p} \cap R^G) > 1\} = \{RL_i \mid 1 \leqslant i \leqslant n\}.$$

Each 1-cocycle $\delta_i \in Z^1(\mathscr{T}_i, k^*) = X_k(\mathscr{T}_i)$, which is defined by $\delta_i(\sigma) = \sigma(L_i)/L_i$ ($\sigma \in \mathscr{T}_i$), coincides with the homomorphism

$$\det\colon \mathscr{T}_i \ni \sigma \mapsto [\text{determinant of } \sigma] \in k^*.$$

Now this theorem is a special case of Theorem 2.9.

COROLLARY 3.2. *If $p = 0$ or $(|G|, p) = 1$, then the following statements are equivalent:*

(1) *R^G is a Gorenstein ring.*

(2) *$f_{\det^{-1}}$ is a $\det^{-1}$-invariant of G where $\det^{-1} \in X_k(G)$ stands for the homomorphism*

$$G \ni \sigma \mapsto [\textit{determinant of } \sigma]^{-1} \in k^*.$$

Proof. This can be shown as in the proof of [9, (2.4)] (the results of Watanabe [11, 12] is essential in the proof of this).

Let $\mathscr{R}'(G)$ be the subgroup of G generated by all pseudo-reflections in G and recall that $\mathscr{D}_k(G) = \bigcap_{\chi \in X_k(G)} \operatorname{Ker} \chi$.

PROPOSITION 3.3. *The homomorphism*

$$s\colon X_k(G) \ni \chi \mapsto (\det^{s_i(\chi)})_{1 \leqslant i \leqslant m} \in \bigoplus_{1 \leqslant i \leqslant m} X_k(\mathscr{T}_i)$$

is surjective and $e_1 e_2 \cdots e_m$ is equal to the cardinality of the set consisting of all linear characters χ of G in k^* such that R_χ are free R^G-modules. Furthermore the following conditions are equivalent:

(1) *s is an isomorphism.*

(2) $G = \mathscr{R}'(G)\mathscr{D}_k(G)$.

(3) *For all $\chi \in X_k(G)$, R_χ are free R^G-modules.*

This proposition follows immediately from Proposition 2.5, Corollary 2.8 and Theorem 2.11.

COROLLARY 3.4. *If G is generated by pseudo-reflections in $GL(V)$, then we have $X_k(G) = X_{\bar{k}}(G)$ where $\bar{k}$ is the algebraic closure of k.*

Proof. We apply Proposition 3.3 to the natural $\bar{k}G$-module $\bar{k} \otimes_k V$ and then $X_{\bar{k}}(G)$ is isomorphic to $\bigoplus_{1 \leqslant i \leqslant m} \mathbb{Z}/e_i\mathbb{Z}$. Thus, the assertion follows from Proposition 3.3.

PROPOSITION 3.5. *Let A be a subring of k with k as the quotient field and assume that A is a Krull domain. Let W be an A-free AG-submodule of V which generates V as a vector space over k and let B be the symmetric algebra of W over A. If $G = \mathscr{R}'(G)\mathscr{D}_k(G)$, then the natural homomorphism $\alpha\colon \mathrm{Cl}(B^G) \to \mathrm{Cl}(B)$ is injective.*

Proof. Since $U(A) = U(B)$ and G acts trivially on k, we have $H^1(G, U(B)) = Z^1(G, U(A))$ and $H^1(G, U(R)) = Z^1(G, k^*)$. Hence, the canonical homomorphism $\beta\colon H^1_B(G, U(B)) \to H^1(G, k^*)$ is injective and the image of β is contained in $H^1_R(G, k^*)$. By Lemma 2.4 and Proposition 3.3 we get

$$\operatorname{Ker} \alpha \cong H^1_B(G, U(B)) = (0).$$

Propositions 3.3 and 3.5 are generalizations of main results of [3].

PROPOSITION 3.6. *Suppose that k is algebraically closed and G is a solvable group with $|G| \in k^*$. If R^G is factorial, then R^G is a polynomial ring.*

Proof. Assume that R^G is factorial. Then by Corollary 2.12 we see that G is generated by pseudo-reflections in $GL(V)$, and hence R^G is a polynomial ring (cf. [8]).

Hereafter we suppse that R^G is a polynomial ring (notice that $\mathrm{char}(k) = p$ is arbitrary). Then G is generated by pseudo-reflections in $GL(V)$ (cf. [8]). Let N be a normal subgroup of G such that G/N is abelian. Furthermore we assume that $(|G/N|, p) = 1$ if $p > 0$. By the character theory of finite abelian groups we see that $N = \bigcap_{\chi \in \Lambda} \operatorname{Ker} \chi$ for a subgroup Λ of $X_k(G)$ (cf. 3.4). Since $X_k(G/N) = X_{\bar{k}}(G/N)$, every irreducible kG/N-module is one dimensional, and hence there is a natural isomorphism

$$\Theta\colon R^N \to \bigoplus_{\chi \in \Lambda} R_\chi$$

of graded R^G-modules. Let $\bar{s}: X_k(G) \to GL_m(k)$ denote the homomorphism defined by $\bar{s}(\chi) = \mathrm{diag}(\bar{s}_1(\chi),..., \bar{s}_m(\chi))$ for $\chi \in X_k(G)$ where $\bar{s}_i(\chi)$ is the image of $s_i(\chi) \bmod e_i$ under a fixed embedding $\mathbb{Z}/e_i\mathbb{Z} \subsetneq k^*$ as groups ($\mathbb{Z}/e_i\mathbb{Z}$ can be embedded in k^*) ($\mathrm{diag}(a_1,..., a_m)$ stands for the matrix

$$\begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_m \end{pmatrix}$$

which is diagonal).

Lemma 3.7. *There is an isomorphism*

$$\eta: G^{ab}/(G^{ab})_p \to X_k(G)$$

of groups such that for any element σ of $\mathscr{T}_i$ $(1 \leqslant i \leqslant n)$

$$\begin{aligned} \bar{s}_j(\eta(\sigma)) &= \det \sigma \qquad \textit{if} \quad U_i \sim U_j \\ &= 1 \qquad\qquad \textit{otherwise} \end{aligned} \qquad (1 \leqslant j \leqslant m).$$

Proof. Let σ_i be an element of $\mathscr{T}_i$ whose canonical image in $\mathscr{T}_i/\mathscr{E}_i$ is a generator of $\mathscr{T}_i/\mathscr{E}_i$ (recall that $\mathscr{T}_i/\mathscr{E}_i$ is cyclic) and let $\xi: \mathscr{T}_1/\mathscr{E}_1 \oplus \mathscr{T}_2/\mathscr{E}_2 \oplus \cdots \oplus \mathscr{T}_m/\mathscr{E}_m \to G^{ab}/(G^{ab})_p$ be a homomorphism defined by

$$\xi((\underbrace{1,..., 1}_{(i-1)\text{times}}, \sigma_i\mathscr{E}_i, 1,..., 1)) = \sigma_i[G, G](G^{ab})_p \qquad (1 \leqslant i \leqslant m).$$

For each $1 \leqslant i \leqslant m$, by Proposition 3.3 we can find a linear character χ of G such that $s_i(\chi) = 1$ and $\{j \mid 1 \leqslant j \leqslant m, s_j(\chi) \neq 0\} = \{i\}$. If $(\sigma_1^{a_1}\mathscr{E}_1,..., \sigma_m^{a_m}\mathscr{E}_m)$ is contained in Ker ξ for some integers a_i, then we have

$$\begin{aligned} \chi(\sigma_1^{a_1}\mathscr{E}_1,..., \sigma_m^{a_m}\mathscr{E}_m) &= \chi(\sigma_i)^{a_i} \\ &= (\det \sigma_i)^{a_i} \\ &= 1. \end{aligned}$$

Therefore, ξ is a monomorphism. G is generated by pseudo-reflections in $GL(V)$ and, hence, ξ is an isomorphism (cf. Proposition 3.3). On the other hand it follows from the definition of $\bar{s}$ that

$$\mathrm{Im}\, \bar{s} = \bigoplus_{1 \leqslant i \leqslant m} \langle \mathrm{diag}(\underbrace{1,..., 1}_{(i-1)\text{times}}, \det \sigma_i, 1,..., 1)\rangle.$$

Let $\gamma: \mathscr{I}_1/\mathscr{E}_1 \oplus \cdots \oplus \mathscr{I}_m/\mathscr{E}_m \to \operatorname{Im} \bar{s}$ be a homomorphism such that

$$\gamma((\underbrace{1,\dots,1}_{(i-1)\text{times}}, \sigma_i\mathscr{E}_i, 1,\dots,1)) = \operatorname{diag}(\underbrace{1,\dots,1}_{(i-1)\text{times}}, \det\sigma_i, 1,\dots,1).$$

Then γ is bijective and $\eta = \bar{s}^{-1}\gamma\xi^{-1}$ is an isomorphism as desired.

We now define a homomorphism $\rho: G \to GL_m(k)$ such that the diagram

$$\begin{tikzcd} X_k(G) \arrow[r, "\bar{s}"'] & GL_m(k) \\ G^{ab}/(G^{ab})_p \arrow[u, "\eta"] & G \arrow[l, "\text{can.}"] \arrow[u, "\rho"'] \end{tikzcd}$$

is commutative.

THEOREM 3.8. *R^N is a complete intersection if and only if $\rho(N)$ coincides with the group $G_D(k)$ in $GL_m(k)$ for some datum D (see* [13], *for definition of $G_D(k)$ and D).*

We shall prove this theorem in several steps.

(3.9) Let S be an m-dimensional polynomial ring $k[X_1,\dots, X_m]$ over k on which $GL_m(k)$ acts in the natural way. For any element $a = (a_1,\dots, a_m) \in \mathbb{Z}_+^m$, X^a stands for the monomial $X_1^{a_1}\cdots X_m^{a_m}$ in S. Clearly $\rho(G)$ is a diagonal group and we have $S^{\rho(G)} = k[X_1^{e_1},\dots, X_m^{e_m}]$.

(3.10) *$S^{\rho(N)}$ is generated by*

$$\{X_1^{e_1},\dots, X_m^{e_m}\} \cup \{X^{\bar{s}(\chi)} \mid \chi \in \Lambda\}$$

as a k-algebra where $\bar{s}(\chi) = (s_1(\chi),\dots, s_m(\chi))$.

Proof. For any element $a = (a_1,\dots, a_m) \in \mathbb{Z}_+^m$, X^a is an invariant of $\rho(G)$ relative to a linear character ψ. Then $X^{a'}$ is contained in S_ψ if $a' = a'_1,\dots, a'_m) \in \mathbb{Z}_+^m$ satisfies that $a_i \equiv a'_i \bmod e_i$ and $a'_i < e_i$ $(1 \leqslant i \leqslant m)$. Since G is generated by pseudo-reflections in $GL(V)$, for $\tau \in \rho(N)$ we can choose pseudo-reflections τ_i from G such that $\tau = \rho(\tau_1 \cdots \tau_u)$. Then, by Lemma 3.7, we have

$$\tau(X^a)/X^a (= \tau(X^{a'})/X^{a'}) = \tau_1 \cdots \tau_u(F)/F,$$

where

$$F = \coprod_{1 \leqslant i \leqslant m} \Big(\coprod_{U_j \sim U_i} L_j\Big)^{a'_i}.$$

Hence the condition $\rho(N) \subseteq \operatorname{Ker}\psi$ is equivalent to the condition $F \in R^N$.

Obviously ψ satisfies that $s_j(\psi) = a_i^j$ $(1 \leqslant i \leqslant m;\ 1 \leqslant j \leqslant n)$ when $U_i \sim U_j$. Thus, ψ belongs to Λ if and only if $\rho(N)$ is contained in Ker ψ. Because $S^{\rho(N)}$ is generated by monomials as a k-algebra, we must have

$$S^{\rho(N)} = k[\{X_1^{e_1},..., X_m^{e_m}\} \cup \{X^{\bar{s}(\chi)} \mid \chi \in \Lambda\}].$$

For a graded algebra $A = \bigoplus_{i \geqslant 0} A_i$, A_+ denotes the irrelevant ideal $\bigoplus_{i>0} A_i$ of A.

(3.11) *There is a natural isomorphism*

$$R^N/R_+^G R^N \simeq S^{\rho(N)}/S_+^{\rho(G)} S^{\rho(N)}$$

of k-algebras.

Proof. Using the isomorphism Θ, we can identify $R^N/R_+^G R^N$ with the k-algebra $\bigoplus_{\chi \in \Lambda} kf_\chi \bmod R_+^G R^N$ whose multiplication rule is defined by

$$\begin{aligned} f_{\chi_1} \bmod R_+^G R^N \cdot f_{\chi_2} \bmod R_+^G R^N &= f_{\chi_1\chi_2} \bmod R_+^G R^N \qquad &&\text{if} \quad s_i(\chi_1) + s_i(\chi_2) < e_i \\ &= 0 &&\text{otherwise.} \end{aligned}$$

Then the k-linear homomorphism

$$\begin{array}{ccc} R^N/R_+^G R^N & \to & S^{\rho(N)}/S_+^{\rho(G)} S^{\rho(N)} \\ \Uparrow & & \Uparrow \\ \sum a_\chi f_\chi \bmod R_+^G R^N & \mapsto & \sum a_\chi X^{\bar{s}(\chi)} \bmod S_+^{\rho(G)} S^{\rho(N)} \end{array}$$

is a k-algebra isomorphism where a_χ are elements of k (cf. (3.10)). Hence the assertion follows.

(3.12) Since R^N (resp. $S^{\rho(N)}$) is a finitely generated graded free R^G-module (resp. $S^{\rho(G)}$-module) and R^G (resp. $S^{\rho(G)}$) is a polynomial ring over k, R^N (resp. $S^{\rho(N)}$) is a Cohen–Macaulay ring. Hence the ideal $R_+^G R^N$ (resp. $S_+^{\rho(G)} S^{\rho(N)}$) is generated by an R^N-regular (resp. $S^{\rho(N)}$-regular) sequence and R^N is a complete intersection if and only if $S^{\rho(N)}$ is a complete intersection. In [13] Watanabe has already determined such a group $\rho(N)$ that $S^{\rho(N)}$ is a complete intersection (i.e., $\rho(N)$ coincides with $G_D(k)$ for some datum D). Thus, the proof of Theorem 3.8 is completed.

ACKNOWLEDGMENT

The author is deeply grateful to Professor S. Endo for suggesting to him improvements of results in Section 2 of an early version of this paper.

References

1. A. Bialynicki-Birula, Remarks on the action of an algebraic torus on K^n, *Polska Acad. Nauk Bull.* **14** (1966), 171–181.
2. N. Bourbaki, "Groupes et algèbres de Lie," Chaps. 4, 5 et 6, Hermann, Paris, 1968.
3. A. Dress, On finite groups generated by pseudo-reflections, *J. Algebra* **11** (1969), 1–5.
4. M. Kang, Picard groups of some rings of invariants, *J. Algebra* **58** (1979), 455–461.
5. T. Molien, Über die Invarianten der linearen Substitutionsgruppen, *Sitzungsber. König Preuss. Akad. Wiss.* (1897), 1152–1156.
6. M. Nagata, "Local Rings," Interscience, New York, 1962.
7. P. Samuel, "Lectures on Unique Factorization Domains," Tata Institute Lecture Notes, Bombay, 1964.
8. J.-P. Serre, Groupes finis d'automorphismes d'anneaux locaux réguliers, *Colloq. Alg. E.N.S.* (1967).
9. R. Stanley, Relative invariants of finite groups generated by pseudo-reflections, *J. Algebra* **49** (1977), 134–148.
10. R. Stanley, Invariants of finite groups and their applications to combinatorics, *Bull. Amer. Math. Soc.* **1** (1979), 475–511.
11. K. Watanabe, Certain invariant subrings are Gorenstein, I, *Osaka J. Math.* **11** (1974), 1–8.
12. K. Watanabe, Certain invariant subrings are Gorenstein, II, *Osaka J. Math.* **11** (1974), 379–388.
13. K. Watanabe, Invariant subrings which are complete intersections, I (Invariant subrings of finite Abelian groups), *Nagoya Math. J.* **77** (1980), 89–98.